AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Rferred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2026)

SmartWSN-IDS: A Hybrid Deep Reservoir and Optimized Tree Model for Routing Attack Detection

P. Bhargavi[1*], Annangi Nishitha[2], Badugu Reethu Sri[2], Kaki Poorna Yamini[2], Kota Vishnu Vardhan Reddy[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Electronics and Communication Engineering

[1,2]Geethanjali Institute of Science and Technology, Nellore-Bombay Highway, S.P.S.R, Andhra Pradesh 524137, India

*Correspondence: P. Bhargavi

ABSTRACT

Wireless Sensor Networks (WSNs) comprise a large number of low-power sensor nodes deployed in applications such as environmental monitoring, healthcare, military surveillance, and smart cities. Recent studies indicate that over 60% of WSN deployments operate in unattended and hostile environments, making them highly susceptible to security threats. This vulnerability has increased the impact of routing attacks, including Time Division Multiple Access (TDMA) attacks, black-hole attacks, flooding attacks, and gray-hole attacks. These attacks significantly degrade network performance by causing packet loss, excessive energy consumption, and delays in communication. Conventional intrusion detection systems (IDS) for WSNs, which rely on manual rules and predefined thresholds, are inadequate for dynamic and large-scale environments. Such approaches depend heavily on expert knowledge and static monitoring mechanisms, resulting in high false alarm rates, poor scalability, delayed detection, and limited adaptability to emerging or hybrid attacks. To address these limitations, this study proposes a Dual Tree Optimizer-based WSN Routing Attack Detection (DTO-WSN-RAD) framework. The framework begins with the utilization of a WSN routing attack dataset, followed by comprehensive data preprocessing steps including normalization, noise removal, and feature selection to improve data quality. For performance benchmarking, existing classification models such as Decision Tree Classifier (DTC), Ridge Classifier (RC), and Linear Discriminant Analysis (LDA) are implemented. The proposed approach integrates Echo State Network (ESN)-based feature extraction with Decision Tree Cost Complexity Pruning (DTCCP) to effectively capture both temporal and structural routing behaviors. This hybrid model enables accurate detection and classification of TDMA, black-hole, flooding, and gray-hole attacks. Experimental results demonstrate that the DTO-WSN-RAD framework achieves higher detection accuracy, improved robustness, and better adaptability compared to conventional methods.

Keywords: Wireless Sensor Networks, Routing Attacks Detection, Echo State Network, Intrusion Detection System, Decision Tree Cost Complexity Pruning.

1. INTRODUCTION

Due to the rapid growth of Internet of Things (IoT) and the services of WSNs, the methodologies for secure communications over the network acquire more attention. The efficient features of sensor networks such as cheaper nodes, fast node deployment and self-organization of nodes play an important role in framing efficient networks and providing a smart communication environment. Moreover, the omnipresent sensor nodes can acquire physical data of the deployed environment and administrate the environment. In the limited range of wireless network communications, the data transmission can be effectively made through the multi hop path transmission. In such a scenario, the model of secure routing protocol that establishes the data transmission path is a significant process that impacts the WSN performance effectively. The general

framework of secure WSN is presented in the Fig. 1.

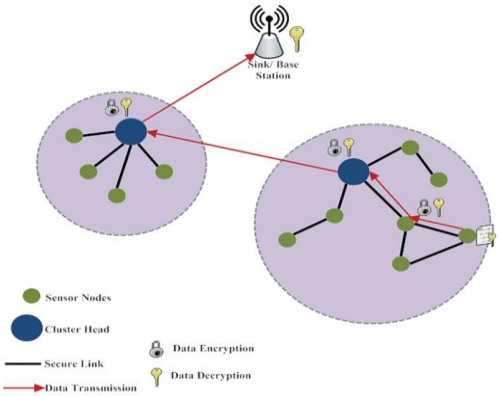


Fig. 1: General framework of secure wireless sensor network model.

The security factors are mainly considered to design an efficient routing protocol in WSNs. The WSNs are open to various attacks, because of their typical features such as, distributed nature, openness and adaptive features of networks. In general, the attacks in WSN can be categorized into, internal and external, which affects network communications through malicious nodes. In recent days, several models have been developed to solve security issues and present mitigation techniques. For enforcing security, cryptographic techniques are used. In utilizing cryptographic primitives, two factors are to be considered as follows,

- The cryptographic functions need higher computational complexities
- Many encryption techniques require central admin to control, which is not applicable in WSN
- When the nodes are distributed in unattended regions they could be attacked by attackers easily.

On focusing the above aspects, developing a model with a defending mechanism and trust management provides optimal solutions. For determining the secure route effectively, the trust management-based evaluations aids to find the security factor of the sensor at next-hop through which the data is transmitted from the source node to the base station. In conventional methods of securing WSN, there exists several key based issues in routing. Moreover, in designing a new model for secure WSN communications, the Quality of Service (QoS) parameters such as the transmission delay and hop counts are to be considered. Models incorporating trust management in WSN include trust evaluations and derivations for proper execution. But, in some cases, the trust management in WSN is registered as a complicated process.

2. LITERATURE SURVEY

Anant Upadhiyay et al. [1] proposed a cyber-resilient framework integrating a modified Ant Colony Optimization routing mechanism with an ensemble Intrusion Detection System (IDS). Their approach utilized CatBoost and XGBoost for distributed intelligence and achieved significant improvements in energy efficiency, latency, and intrusion detection. Walaa N. Ismail et al. [2] introduced a metaheuristic-based IDS framework for 5G networks using a lightweight CNN and attention-based XGBoost model optimized by Cat Swarm Optimization. Their model demonstrated extremely high accuracy with minimal false positives in both binary and multiclass classification. Sreeja Balachandran Nair Premakumari et al. [3] developed a reinforcement learning-based adaptive encryption system that dynamically adjusts encryption strength based on threat levels. Their approach improved energy efficiency while maintaining strong security in WSN environments. Joshua T. Ibibo et al. [4] proposed IbiboRPLChain II, a blockchain-enhanced routing security framework for IoT networks. By integrating smart contracts and decentralized authentication, the model improved packet delivery, reduced delay, and enhanced resilience against routing attacks. Ioana Matei et al. [5] introduced a gateway-based trust evaluation model using decision tree regression for Internet of Battle Things applications. Their system provided real-time trust assessment with improved reliability and low latency.

Abdulla Juwaied et al. [6] enhanced clustering protocols such as LEACH and SEP using a K-Nearest Neighbors algorithm. Their method reduced communication distance and energy consumption while extending network lifetime. Rashid Mustafa et al. [7] proposed a cross-layer IoT security framework combining machine learning-based anomaly detection with lightweight Speck encryption. Their results showed reduced false positives and improved energy efficiency compared to traditional methods. Altaf Hussain et al. [8] developed an energy-efficient and trust-based routing scheme for underwater sensor networks using autonomous underwater vehicles and 6G communication. Their approach improved network lifetime and security performance. Mahsa Mohaghegh et al. [9] proposed a secure cross-layer IoT architecture combining lightweight cryptography and adaptive communication strategies, achieving high packet delivery ratio and reduced energy consumption. Vivek Kumar Pandey et al. [10] introduced a deep learning-based authentication framework for Internet of Drones (IoD), providing resistance against replay, MITM, and impersonation attacks with improved efficiency. Ponnusamy Chinnasamy et al. [11] proposed a blockchain-enabled security framework for 6G WSNs using optimized machine learning techniques, achieving high throughput, energy efficiency, and secure routing. Mbarka Belhaj Mohamed et al. [12] developed the S-2EC-ERF framework integrating enhanced random forest-based attack detection with energy-efficient routing, achieving high detection accuracy and improved network performance. Vasily Desnitsky et al. [13] proposed a decentralized WSN attack detection model using formal modeling and machine learning techniques, achieving high detection accuracy with an F1-score of 0.99. Beibei Wang et al. [14] introduced a dynamic trust evaluation model combining random forest and deep reinforcement learning for underwater sensor networks, significantly improving malicious node detection. Bassey Isong et al. [15] presented a comprehensive review of intrusion detection systems for IoT, highlighting the effectiveness of machine learning and identifying challenges such as scalability, resource constraints, and dataset limitations.

3. PROPOSED SYSTEM

The proposed system architecture is designed to detect routing attacks in WSNs by combining traditional machine learning classifiers with an advanced temporal feature extraction model. The architecture begins with the collection of WSN routing data, followed by preprocessing and exploratory data analysis to improve data quality and understanding. The dataset is then divided into training and testing sets for unbiased evaluation. Existing classifiers such as DTC, RC, and LDA are implemented as baseline models. The core contribution of the architecture is the proposed hybrid model, which integrates ESN based feature extraction with a DTCCP classifier. Finally, the system classifies network behavior into normal and various routing attack categories, enabling accurate and reliable intrusion detection in WSN environments as demonstrated in Fig. 2.

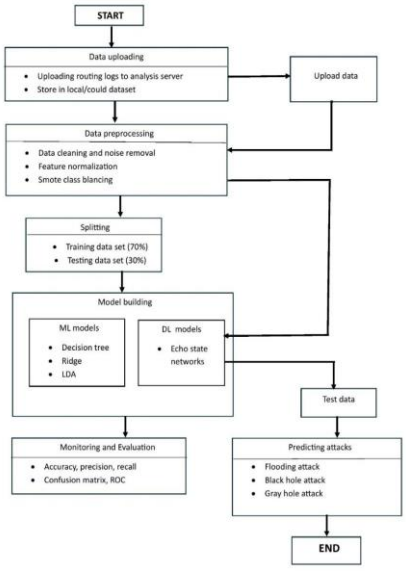


Fig. 2: Proposed system architecture.

WSN Dataset: The WSNs dataset is collected from a simulated or real sensor network environment where multiple sensor nodes communicate using routing protocols. The dataset captures both normal and malicious

routing behaviors by recording network parameters such as packet delivery ratio, packet loss rate, delay, energy consumption, hop count, and TDMA slot timing. Each data instance is labeled according to the observed behavior, including Normal operation, TDMA attacks, gray hole attack Black hole attacks, and other routing-based intrusions.

Data Preprocessing: Data preprocessing is performed to improve the quality and reliability of the WSN dataset before model training. This step involves removing missing, duplicate, and inconsistent records that may arise due to sensor faults or communication errors. Numerical features are normalized or scaled to ensure uniform contribution during learning, while categorical labels are encoded into numerical form. Feature selection techniques may also be applied to eliminate redundant routing parameters, thereby reducing dimensionality and improving computational efficiency.

Exploratory Data Analysis (EDA): EDA is conducted to understand the underlying patterns and statistical properties of the WSN dataset. During this phase, the distribution of normal and attack classes is examined to identify class imbalance issues. Correlation analysis is performed to study the relationship between routing features and different attack types. EDA helps reveal abnormal behaviors such as high packet drops in Blackhole attacks or intermittent losses in gray hole attacks, providing insights that guide effective model selection and feature extraction.

Train–Test Splitting: The preprocessed dataset is divided into training and testing subsets to ensure unbiased evaluation of the classification models. The training set is used to learn decision boundaries and routing behavior patterns, while the testing set is reserved for evaluating model performance on unseen data. A common split ratio such as 70:30 or 80:20 is used to balance learning efficiency and generalization capability. This step ensures that the system avoids overfitting and provides reliable detection results.

Existing Decision Tree Classifier: The existing DTC is trained using the training dataset to establish a baseline detection model. It constructs a tree structure by recursively selecting routing features based on splitting criteria such as Information Gain or Gini Index. The decision tree generates interpretable if–then rules that classify network behavior into normal or attack categories. Although simple and efficient, this model may struggle with complex or overlapping attack patterns in WSN environments.

Existing Ridge Classifier: The Ridge classifier is applied to address multicollinearity among routing features and reduce overfitting. By incorporating L2 regularization, the model penalizes large coefficient values and stabilizes the learning process. Ridge classification assumes linear separability between classes and learns optimal weights for routing parameters. This step evaluates the effectiveness of regularized linear models in detecting routing attacks within WSNs.

Existing LDA Classifier: LDA is employed to project high-dimensional routing data into a lower-dimensional space while preserving maximum class separability. LDA computes discriminant functions based on class means and variances, enabling effective classification of normal and attack behaviors. This approach is particularly useful for understanding how well statistical feature transformations can distinguish between different routing attack types in WSNs.

Proposed ESN Feature Extraction with DTCCP Classifier: In the proposed system, an ESN is used to extract temporal and dynamic features from WSN routing data. ESN captures time-dependent patterns such as TDMA slot violations and gradual packet dropping behavior in Gray hole attacks. The extracted reservoir states are then fed into the DTCCP (Decision Tree Cost Complex Pruning) classifier, which enhances traditional decision

trees by incorporating conditional probabilities and contextual feature dependencies. This hybrid model improves classification accuracy and robustness, especially for complex and stealthy routing attacks.

Output Classes: The final output of the system is the classification of each WSN data instance into predefined categories such as Normal, TDMA attack, Grayhole attack, Blackhole attack, and other routing attacks. The system's performance is evaluated using metrics including accuracy, precision, recall, and F1-score. The classified results enable timely detection of malicious nodes and support effective intrusion response mechanisms to enhance the overall security and reliability of WSNs.

ESN-DTCCP

The proposed system aims to improve the detection of routing attacks in WSNs by combining the strengths of ESN and a DTC optimized using cost-complexity pruning as shown in Fig. 3. WSN environments are highly dynamic due to frequent topology changes, limited node energy, and time-dependent routing behavior. Traditional classifiers rely mainly on static routing features and fail to capture the temporal evolution of attacks such as gray hole, TDMA violations, and selective packet dropping. To overcome these limitations, the proposed system introduces ESN-based temporal feature extraction followed by an optimized decision-tree-based classification mechanism.

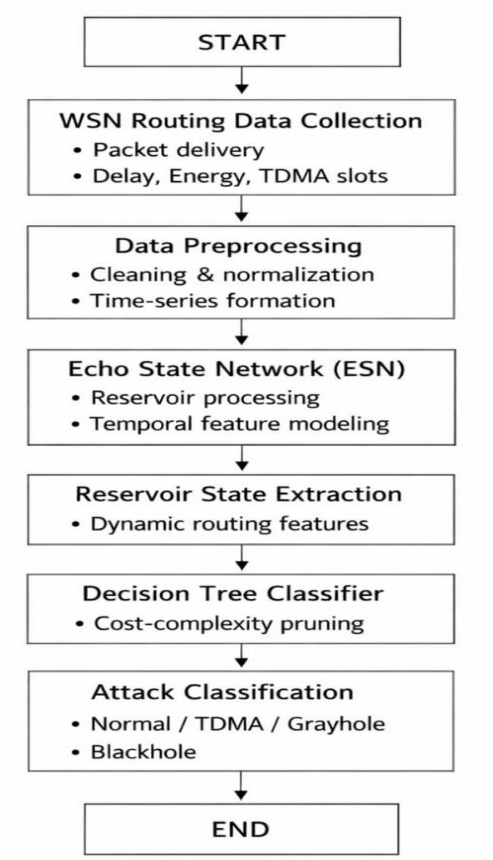


Fig. 3: EST and DTCCP flow chart.

Temporal Modeling Using Echo State Network: The preprocessed data is fed into the ESN. ESN consists of an input layer, a large randomly connected reservoir, and an output layer. The reservoir transforms the input routing features into rich dynamic internal states, capturing temporal dependencies without iterative weight training.

Reservoir State Extraction: The internal reservoir states generated over time are collected and stored as new feature vectors. These features represent dynamic routing behavior, enabling detection of subtle and slow-acting attacks such as Gray hole and TDMA violations.

Decision Tree Training with Cost-Complexity Pruning: The ESN-extracted features are passed to a Decision Tree classifier. Cost-complexity pruning is applied to remove unnecessary branches that contribute little to classification accuracy. This results in a

compact tree that balances model complexity and detection performance.

Classification and Testing: The trained ESN–Decision Tree model is evaluated using unseen WSN data. Each routing instance is classified as Normal or as a specific routing attack such as TDMA, Gray hole, or Black hole based on learned decision rules.

Attack Detection Output: The final output identifies malicious nodes and attack types in the network. This information can be used for intrusion response, routing path isolation, or network reconfiguration to enhance WSN security.

4. RESULTS ANALYSIS

Fig. 4 confusion matrix demonstrates highly accurate classification across five classes—Normal, Flooding, TDMA, Grayhole, and Blackhole. Specifically, 135,981 Normal instances are correctly classified with only 46 misclassified as TDMA, while Flooding attacks achieve 136,016 correct predictions with just 10 misclassified as Grayhole. The TDMA class records 135,985 correct classifications with minimal errors (28 as Normal and 13 as Grayhole). Similarly, Grayhole attacks show 135,907 correct predictions with very few misclassifications, and Blackhole attacks achieve 135,934 correct predictions with negligible errors. These results indicate extremely low misclassification rates across all classes. Furthermore, the ROC curves for all five classes rise sharply toward the top-left corner, achieving a True Positive Rate close to 1.0 with a near-zero False Positive Rate. The Area Under the Curve (AUC) for all classes is reported as 1.00, confirming perfect separability and superior discrimination capability compared to a random classifier. Overall, the results validate that the proposed model achieves near-perfect classification performance with maximum sensitivity and specificity across all attack categories.

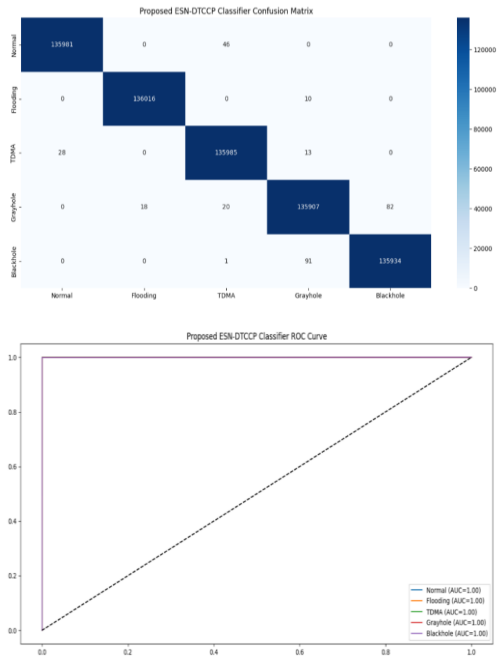


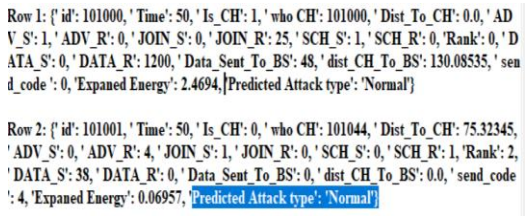
Fig. 4: Confusion matrix and ROC curve of Proposed ENS-DTCCP Classifie.

Table 1 Overall performance comparison table of various WSN attack detection methods.

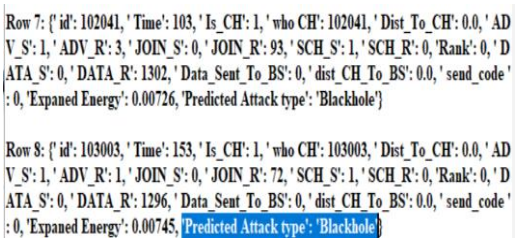
Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
DTC model	39.99	24.98	39.99	27.99
RC model	87.71	89.35	87.71	87.19
LDA model	87.92	89.31	87.92	87.56
Proposed ESN-DTCCP	99.95	99.95	99.95	99.95

Table 1 presents the overall performance comparison of different WSN attack detection methods, including DTC, RC, LDA, and the proposed ESN-DTCCP model. The DTC model shows poor performance, achieving only 39.99% accuracy and low precision, recall, and F1-score, indicating its inability to effectively detect attacks. In contrast, the RC and LDA

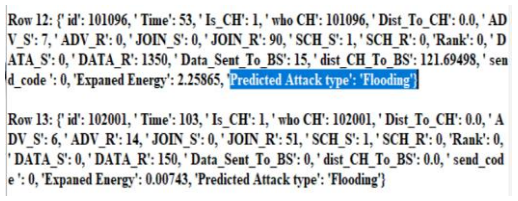
models demonstrate moderate performance, with accuracy values of 87.71% and 87.92%, respectively, along with relatively balanced precision and recall. However, both models still fall short in achieving high reliability for critical security applications. The proposed ESN-DTCCP model significantly outperforms all existing methods, achieving 99.95% across accuracy, precision, recall, and F1-score. This near-perfect performance highlights the robustness and effectiveness of the proposed approach in accurately detecting and classifying WSN attacks.


Row 1: {' id': 101000, ' Time': 50, ' Is_CH': 1, ' who CH': 101000, ' Dist_To_CH': 0.0, ' ADV_S': 1, ' ADV_R': 0, ' JOIN_S': 0, ' JOIN_R': 25, ' SCH_S': 1, ' SCH_R': 0, 'Rank': 0, ' DATA_S': 0, ' DATA_R': 1200, ' Data_Sent_To_BS': 48, ' dist_CH_To_BS': 130.08535, ' send_code ': 0, 'Expaned Energy': 2.4694, 'Predicted Attack type': 'Normal'}
Row 2: {' id': 101001, ' Time': 50, ' Is_CH': 0, ' who CH': 101044, ' Dist_To_CH': 75.32345, ' ADV_S': 0, ' ADV_R': 4, ' JOIN_S': 1, ' JOIN_R': 0, ' SCH_S': 0, ' SCH_R': 1, 'Rank': 2, ' DATA_S': 38, ' DATA_R': 0, ' Data_Sent_To_BS': 0, ' dist_CH_To_BS': 0.0, ' send_code ': 4, 'Expaned Energy': 0.06957, 'Predicted Attack type': 'Normal'}

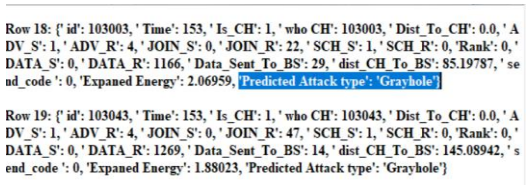
(a)


Row 7: {' id': 102041, ' Time': 103, ' Is_CH': 1, ' who CH': 102041, ' Dist_To_CH': 0.0, ' ADV_S': 1, ' ADV_R': 3, ' JOIN_S': 0, ' JOIN_R': 93, ' SCH_S': 1, ' SCH_R': 0, 'Rank': 0, ' DATA_S': 0, ' DATA_R': 1302, ' Data_Sent_To_BS': 0, ' dist_CH_To_BS': 0.0, ' send_code ': 0, 'Expaned Energy': 0.00726, 'Predicted Attack type': 'Blackhole'}
Row 8: {' id': 103003, ' Time': 153, ' Is_CH': 1, ' who CH': 103003, ' Dist_To_CH': 0.0, ' ADV_S': 1, ' ADV_R': 1, ' JOIN_S': 0, ' JOIN_R': 72, ' SCH_S': 1, ' SCH_R': 0, 'Rank': 0, ' DATA_S': 0, ' DATA_R': 1296, ' Data_Sent_To_BS': 0, ' dist_CH_To_BS': 0.0, ' send_code ': 0, 'Expaned Energy': 0.00745, 'Predicted Attack type': 'Blackhole'}

(b)


Row 12: {' id': 101096, ' Time': 53, ' Is_CH': 1, ' who CH': 101096, ' Dist_To_CH': 0.0, ' ADV_S': 7, ' ADV_R': 0, ' JOIN_S': 0, ' JOIN_R': 90, ' SCH_S': 1, ' SCH_R': 0, 'Rank': 0, ' DATA_S': 0, ' DATA_R': 1350, ' Data_Sent_To_BS': 15, ' dist_CH_To_BS': 121.69498, ' send_code ': 0, 'Expaned Energy': 2.25865, 'Predicted Attack type': 'Flooding'}
Row 13: {' id': 102001, ' Time': 103, ' Is_CH': 1, ' who CH': 102001, ' Dist_To_CH': 0.0, ' ADV_S': 6, ' ADV_R': 14, ' JOIN_S': 0, ' JOIN_R': 51, ' SCH_S': 1, ' SCH_R': 0, 'Rank': 0, ' DATA_S': 0, ' DATA_R': 150, ' Data_Sent_To_BS': 0, ' dist_CH_To_BS': 0.0, ' send_code ': 0, 'Expaned Energy': 0.00743, 'Predicted Attack type': 'Flooding'}

(c)


Row 18: {' id': 103003, ' Time': 153, ' Is_CH': 1, ' who CH': 103003, ' Dist_To_CH': 0.0, ' ADV_S': 1, ' ADV_R': 4, ' JOIN_S': 0, ' JOIN_R': 22, ' SCH_S': 1, ' SCH_R': 0, 'Rank': 0, ' DATA_S': 0, ' DATA_R': 1166, ' Data_Sent_To_BS': 29, ' dist_CH_To_BS': 85.19787, ' send_code ': 0, 'Expaned Energy': 2.06959, 'Predicted Attack type': 'Grayhole'}
Row 19: {' id': 103043, ' Time': 153, ' Is_CH': 1, ' who CH': 103043, ' Dist_To_CH': 0.0, ' ADV_S': 1, ' ADV_R': 4, ' JOIN_S': 0, ' JOIN_R': 47, ' SCH_S': 1, ' SCH_R': 0, 'Rank': 0, ' DATA_S': 0, ' DATA_R': 1269, ' Data_Sent_To_BS': 14, ' dist_CH_To_BS': 145.08942, ' send_code ': 0, 'Expaned Energy': 1.88023, 'Predicted Attack type': 'Grayhole'}

(d)

Fig. 5: Predictions on test data. (a) normal, (b) blackhole attack, (c) flooding attack, (d) grayhole attack.

Fig. 5 (a) shows the prediction results generated by the proposed ESN–DTCCP classifier on test instances of the WSN dataset. The output displays detailed feature values for each node along with the predicted attack type. For example, in Row 1, node id 101000 at Time 50 is identified as a Cluster Head (Is_CH = 1) with Dist_To_CH = 0.0, DATA_R = 1200, Data_Sent_To_BS = 48, dist_CH_To_BS = 130.08535, and energy consumption of 2.4694 units, and the model correctly predicts the attack type as “Normal.” Similarly, Row 2 shows node id 101001 operating as a member node (Is_CH = 0) with Dist_To_CH = 75.32345, DATA_S = 38, DATA_R = 0, Data_Sent_To_BS = 0, and Expended Energy = 0.06957, which is also classified as “Normal.” The displayed results confirm that the classifier evaluates multiple routing parameters such as advertisement packets (ADV_S, ADV_R), join requests (JOIN_S, JOIN_R), scheduling packets (SCH_S, SCH_R), rank, and energy metrics before assigning a class label. The accurate prediction of “Normal” for these instances demonstrates the effectiveness of the proposed model in correctly identifying legitimate routing behavior based on both communication and energy-related features.

Fig. 5 (b) shows the prediction results of the proposed ESN–DTCCP classifier for malicious routing behavior, specifically Blackhole attacks. In Row 7, node id 102041 at Time 103 is identified as a Cluster Head (Is_CH = 1) with Dist_To_CH = 0.0 and a high DATA_R value of 1302 packets, while Data_Sent_To_BS = 0 and dist_CH_To_BS = 0.0, indicating that although the node receives a large amount of data, it does not forward any packets to the Base Station. The node also records JOIN_R = 93 and Expended Energy = 0.00726, yet fails to transmit aggregated data, which is a strong indicator of Blackhole behavior. Similarly, Row 8 shows node id 103003 at Time 153 acting as a Cluster Head with DATA_R = 1296, JOIN_R = 72, Data_Sent_To_BS = 0, and Expended Energy = 0.00745, again demonstrating that the node receives substantial traffic but drops packets instead of forwarding

them. Based on these abnormal routing characteristics—high data reception, zero forwarding, and minimal energy usage—the model correctly predicts the attack type as "Blackhole" for both instances, confirming the effectiveness of the proposed hybrid framework in detecting packet-dropping attacks in WSN environments.

Fig. 5 (c) shows the prediction results of the proposed model for Flooding attacks in the WSN environment. In Row 12, node id 101096 at Time 53 is acting as a Cluster Head (Is_CH = 1) with ADV_S = 7 and a very high DATA_R value of 1350 packets, but it forwards only 15 packets to the Base Station (Data_Sent_To_BS = 15) despite having a significant distance to the BS (dist_CH_To_BS = 121.69498). The node also records JOIN_R = 90 and an Expended Energy of 2.25865, indicating abnormal excessive communication activity, which is characteristic of flooding behavior. Similarly, Row 13 shows node id 102001 at Time 103 with ADV_S = 6, ADV_R = 14, JOIN_R = 51, and DATA_R = 150, yet Data_Sent_To_BS = 0 and dist_CH_To_BS = 0.0, reflecting irregular packet handling and unnecessary control message transmission. The combination of high advertisement transmissions, abnormal packet reception patterns, and inefficient forwarding confirms malicious flooding activity. Based on these routing and traffic anomalies, the classifier accurately predicts the attack type as "Flooding" for both instances, demonstrating its capability to detect excessive packet injection attacks effectively.

Fig. 5 (d) shows the prediction results of the proposed framework for detecting Grayhole attacks in the wireless sensor network. In Row 18, node id 103003 at Time 153 operates as a Cluster Head (Is_CH = 1) with DATA_R = 1166 packets received, but forwards only 29 packets to the Base Station (Data_Sent_To_BS = 29) despite having a moderate distance to the BS (dist_CH_To_BS = 85.19787). The node also records ADV_S = 1, ADV_R = 4, JOIN_R = 22, and Expended Energy = 2.06959, indicating selective forwarding behavior rather than complete dropping.

5. Conclusion

The proposed WSN-RAD with ESN–DTCC framework demonstrates significant improvement over traditional machine learning classifiers. From the experimental results, the DTC achieved only 39.99% accuracy with a macro F1-score of 0.28, showing severe misclassification issues, particularly for Normal, Grayhole, and Blackhole attacks. In contrast, the Ridge and LDA classifiers achieved improved performance with accuracies of 87.71% and 87.92%, respectively, and macro F1-scores of 0.87 and 0.88. However, both models showed moderate weakness in detecting TDMA attacks, with recall values of 0.56 (Ridge) and 0.59 (LDA). The proposed ESN–DTCCP classifier significantly outperformed all existing models by achieving 99.95% accuracy, 99.95% precision, 99.95% recall, and 99.95% F1-score, with perfect class-wise detection (1.00) across Normal, Flooding, TDMA, Grayhole, and Blackhole categories. The integration of ESN for temporal feature extraction with Decision Tree Cost-Complexity Pruning (DTCCP) enabled the system to capture dynamic routing behaviors and subtle attack patterns that static classifiers failed to detect. The model also achieved perfect macro and micro averages of 1.00, demonstrating balanced and unbiased classification performance across all 680,132 instances in the dataset. These results confirm that the proposed hybrid framework is highly robust, reliable, and suitable for real-time routing attack detection in WSNs environments, significantly enhancing network security and reliability.

References

[1] Upadhiyay and A. Jain, "Cyber resilient framework with energy efficient swarm routing and ensemble threat detection in fog assisted WSNs," *Scientific Reports*, vol. 15, 36461, 2025.

[2] W. N. Ismail, "A novel metaheuristic-based methodology for attack detection in wireless communication networks," *Mathematics*, vol. 13, no. 1736, 2025.

[3] S. B. N. Premakumari *et al.*, "Reinforcement Q-learning-based adaptive encryption model for cyberthreat mitigation in WSNs," *Sensors*, vol. 25, no. 2056, 2025.

[4] J. T. Ibibo *et al.*, "IbiboRPLChain II: A blockchain-enhanced security framework for mitigating routing attacks in IoT-RPL networks," *Applied Sciences*, vol. 15, no. 11874, 2025.

[5] I. Matei and V.-V. Patriciu, "A decision tree regression algorithm for real-time trust evaluation of battlefield IoT devices," *Algorithms*, vol. 18, no. 641, 2025.

[6] A. Juwaied *et al.*, "Enhancing clustering efficiency in heterogeneous WSNs protocols using the K-nearest neighbours algorithm," *Sensors*, vol. 25, no. 1029, 2025.

[7] R. Mustafa *et al.*, "Cross-layer analysis of machine learning models for secure and energy-efficient IoT networks," *Sensors*, vol. 25, no. 3720, 2025.

[8] A. Hussain *et al.*, "Energy-efficient and trust-based autonomous underwater vehicle scheme for 6G-enabled Internet of underwater things," *Sensors*, vol. 25, no. 286, 2025.

[9] R. Mustafa *et al.*, "A secure and energy-efficient cross-layer network architecture for the Internet of Things," *Sensors*, vol. 25, no. 3457, 2025.

[10] V. K. Pandey *et al.*, "An efficient framework for secure communication in Internet of drone networks using deep computing," *Designs*, vol. 9, no. 61, 2025.

[11] P. Chinnasamy *et al.*, "Blockchain 6G-based wireless network security management with optimization using machine learning techniques," *Sensors*, vol. 24, no. 6143, 2024.

[12] M. B. Mohamed *et al.*, "A security-enhanced energy conservation with enhanced random forest classifier for low execution time framework (S-2EC-ERF) for WSNs," *Applied Sciences*, vol. 14, no. 2244, 2024.

[13] V. Desnitsky and A. Meleshko, "The modeling and detection of attacks in role-based self-organized decentralized WSNs," *Telecom*, vol. 5, pp. 145–175, 2024.

[14] Wang *et al.*, "A dynamic trust model for underwater sensor networks fusing deep reinforcement learning and random forest algorithm," *Applied Sciences*, vol. 14, no. 3374, 2024.

[15] Isong *et al.*, "Insights into modern intrusion detection strategies for Internet of Things ecosystems," *Electronics*, vol. 13, no. 2370, 2024.